ASIGNATURA: LABORATORIO DE HARDWARE

CURSO: 5°3 B

PROFESOR: DAVID JIMENEZ

TEMA: CONFIGURACIÓN DE ROUTERS, SERVIDOR PROXI

Router es un término en inglés que traducido al español quiere decir ruteador o enrutador. Se define como router aquel componente de hardware que logra crear una conexión en los ordenadores a nivel de red. Su forma de funcionar se basa en el envío o encamino de paquetes de datos de una determinada red a otra. Está encargado de distribuir en diversos dispositivos la señal de internet.

Un router es considerado como un tipo de GPS que transfiere o encamina los datos, donde escoge el mejor camino para ello acorde al tráfico.

TIPOS DE ROUTER

Router por cable

Es uno de los tipos de routers de mayor antigüedad, por ello hoy día está en desuso, donde solo se emplea en instalaciones grandes por cables.

Router inalámbrico

También se conoce como **router mixto**. Este puede funcionar sin necesitar cableado, posee diversas salidas y una conectividad wifi, la cual ofrece diversas conexiones de excelente calidad.

Tipos de router inalámbricos

- **Router monobanda**: estos poseen la capacidad para trabajar a 2.4 Ghz, que es la frecuencia más saturada y habitual en la actualidad. Ofrece una velocidad de 450 Mbits/s.
- **Routers 4G**: con estos se obtiene internet inalámbrico sin estar conectado a una línea fija, sea esta de fibra óptica o telefónica. Estos emplean la misma señal 4G de telefonía móvil para señal por cable o por wifi a la casa. Este es de gran utilidad en zonas rurales donde no haya disponibilidad para conectarse a una línea fija.
- **Routers multibanda:** ofrecen una capacidad para trabajar desde 2.4 Ghz y de 5 Ghz, la banda más alta brinda una velocidad superior de 1750 Mbits/s. De estos existen muchos modelos

que brindan diversas posibilidades y rangos de coberturas, ya que posee una mayor cantidad de antenas.

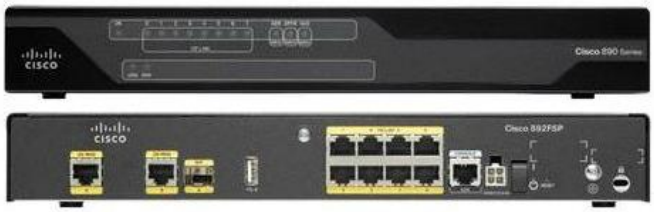
TIPOS DE ROUTER SEGÚN SU USUARIO

Router para uso del consumidor

Es el tipo de router que se usa en las viviendas y en ciertos negocios o empresas de pequeñas dimensiones, los cuales funcionan como punto de acceso inalámbrico para crear una conexión a internet y a otros equipos de configuración local. Se configuran a través de una interface gráfica con menús.

Routers para uso empresarial

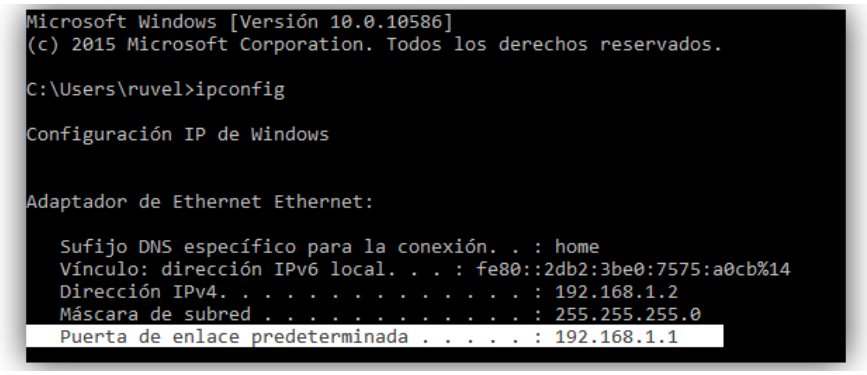
Este tipo de routers llega a ser mucho más rápido y sobre todo potente, siendo útil en el uso empresarial ya que presentan un mayor número de prestaciones y servicios que un router de uso doméstico. Su configuración se realiza a través de comandos de consola lo cual los hace más difíciles de configurar.



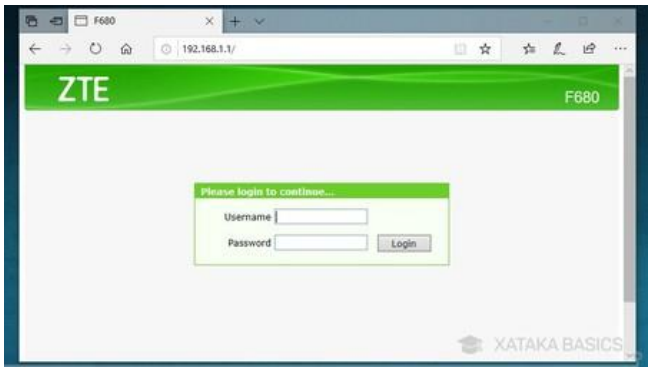
CONFIGURACIÓN DE UN ROUTER

Vamos a tomar como ejemplo la configuración de un router de la marca ZTE. Este es un router de uso doméstico por lo tanto tiene una interface gráfica con menús para su configuración.

Lo primero que debemos hacer es saber la dirección IP del router; para ello ejecutaremos un comando en nuestra consola de DOS. Nos vamos a INICIO, EJECUTAR y tecleamos cmd. Se nos abrirá la consola de DOS. En la consola DOS tecleamos el comando IPCONFIG y le damos ENTER. Se desplegarán varios datos de direcciones IP. A nosotros nos interesa saber la dirección de la “Puerta de enlace predeterminada”; esa es la dirección de nuestro router.

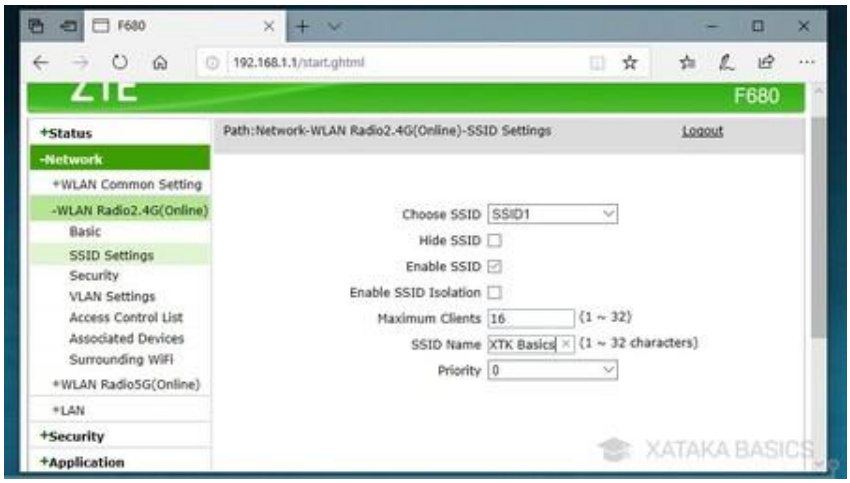


Una vez que tenemos la dirección IP de nuestro router abrimos nuestro navegador e ingresamos en la barra de búsqueda la dirección IP del router 192.168.1.1
Esos números representan la puerta de entrada al panel de administrador del router de la mayoría de los operadores. No pongas ni http, ni nada, sólo los números que componen la IP.



Introduciendo esta dirección te aparecerá una ventana en la que te pedirá el nombre de usuario y la contraseña de tu router para poder acceder a él. Si nunca la has cambiado, mira a ver en las instrucciones, en una pegatina en tu router o buscando el modelo por Internet. En el caso de que no la encuentres y sea el router de un operador, llama a ese operador para que te la diga. El usuario y contraseña suelen ser peligrosamente fáciles, como admin admin, o 1234 1234.

CAMBIAR EL NOMBRE DE LA RED WIFI



Para ello, navega por los menús de tu router hasta **encontrar el apartado *Nombre de red (SSID)***, que es el nombre con el que aparecerá tu WiFi cuando intentes conectarte a ella. En algunos routers puede estar en el apartado *Inalámbrico*, en *Network* u otros similares.

Una vez en el apartado, **tienes que cambiar este nombre SSID predeterminado por uno que tú elijas**. El nombre que pongas es el que verás en tus dispositivos cuando les indiques que empiecen a buscar redes WiFi, o sea que asegúrate de que sea uno que reconozcas y diferente a los demás.

Si tu router es moderno puede que sea de doble banda, y que genere dos redes WiFi de WiFi 2.4G y la 5G. En estos casos, tendrás que cambiarle el nombre SSID a ambas, y acuérdate de hacerlo **de tal**

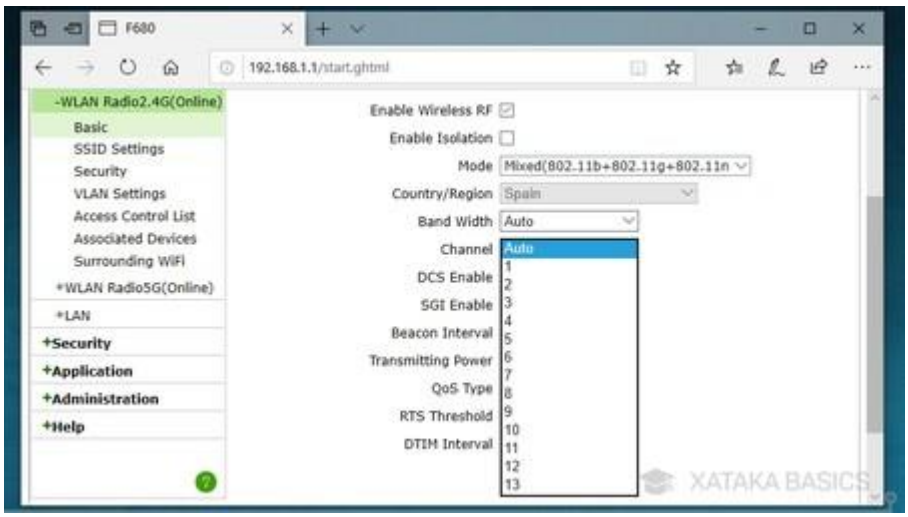
manera que puedas diferenciar ambas bandas. De esta manera, dependiendo de las necesidades de tu dispositivo podrás escoger conectarte a una u otra.

CAMBIAR LA CONTRASEÑA DE LA WIFI

Una vez cambiado el nombre de tu conexión WiFi, el siguiente paso es el de cambiar la clave precompartida de WPA. En algunos routers este parámetro vendrá en algún apartado *Security* dentro de la configuración del WLAN o WiFi. La clave es que **tienes que dar con el término WPA**, que es el nombre técnico que recibe la contraseña de tu WiFi.

A la hora de elegir contraseña, recuerda que **tienes que hacerla lo más robusta posible**, que no sea fácil para que tus vecinos no puedan adivinarla, pero a ser posible que te puedas acordar de ella para no tener que buscar un papelito al conectarte.

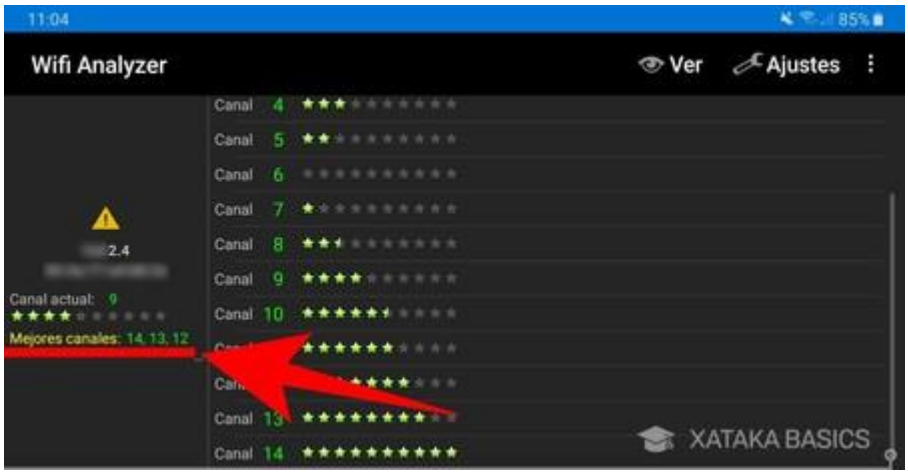
ELIGE EL CANAL DE WIFI



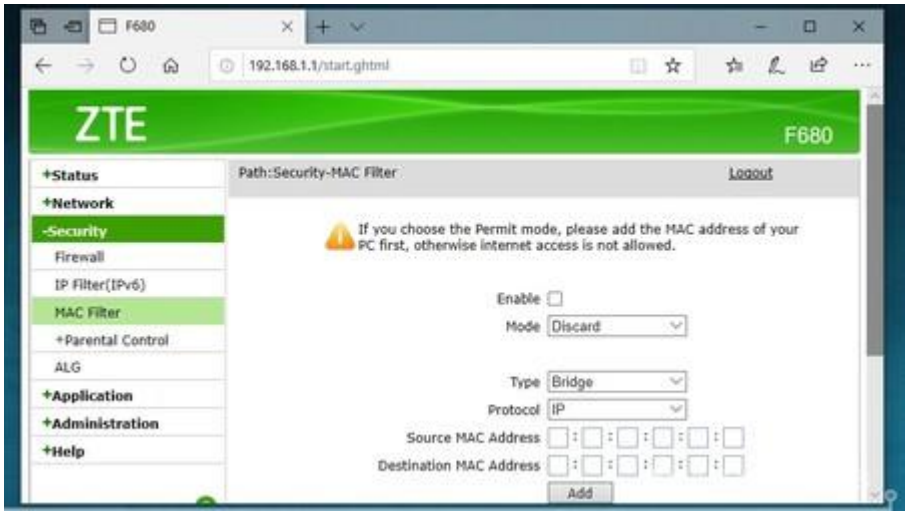
Y ahora que ya tienes hecha la configuración inicial, **puedes cambiar el canal de la WiFi para usar el que más velocidad ofrezca**. Esto no depende tanto del canal como de cuál de ellos esté menos saturado y utilizado por los dispositivos tuyos y de tus vecinos. Las opciones para elegir el canal deberían estar en la configuración de la WiFi, y si es de doble banda, habrá una configuración de canal para tu WLAN de 2.4G y otro para la de 5G.

El router seguramente esté preconfigurado para buscar un canal de forma automática, lo que es suficiente para la mayoría de los casos. Pero si notas que de repente la conexión empieza a ir mal**,** puede que sea porque el canal al que se ha conectado se haya saturado, y en ese caso puede ser útil establecer a mano el canal al que entrar.

La manera más sencilla para comprobar la saturación de canales y decidir cuál utilizar es mediante aplicaciones que permitan su escaneo, como WiFi Analyzer de Android. Es fácil de utilizar, sólo tienes que abrir la app, pulsar en *Ver* y analizar los canales para que te haga **un ranking con los que más libres estén**.



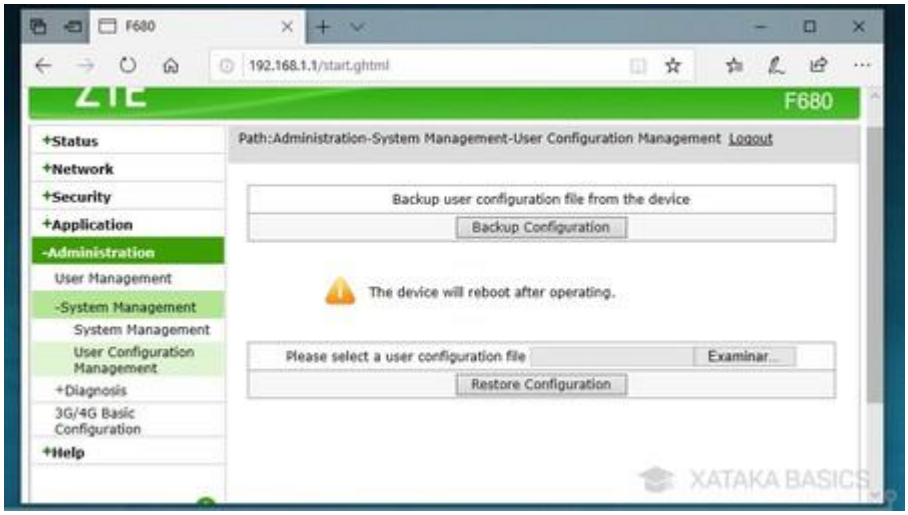
FILTRAR UNA DIRECCIÓN MAC



Si lo que buscas es seguridad, para proteger tu WiFi de que dispositivos indeseados se conecten puedes establecer un filtrado de direcciones MAC. Este es el nombre que se le da al identificador único que tiene cada dispositivo, y permite hacer que determinados dispositivos no puedan conectarse o que sólo los que tu decidas puedan hacerlo.

Para establecer este filtro tienes que **buscar una opción llamada *MAC Filter***, y pulsar en *Enabled* para activarlo. Entonces, puedes añadir direcciones MAC y decidir si quieres que estas estén descargadas y no puedan conectarse o permitidas. La opción *MAC Filter* puede estar en las opciones de seguridad o incluso la configuración *Wireless* de tu router, todo depende del modelo.

COPIA DE SEGURIDAD DE TU CONFIGURACIÓN



Y por último, habrá routers que también te permitan **hacer una copia de seguridad de tu configuración**. Si te has pasado un par de horas configurando a tu medida tu WiFi, está claro que lo que menos quieres es perderlo todo y tenerlo que volver a hacer si por alguna razón falla algo y tienes que resetearlo. Es aquí donde entra la posibilidad de hacer una *Backup* o copia de seguridad que luego puedas restaurar.

Les comparto un link en donde están explicados casi todos los parámetros más importantes en la configuración de un router de marca TPLINK https://www.youtube.com/watch?v=PM_Exu1TiHY

¿QUÉ SON LOS SERVIDORES PROXY Y COMO TRABAJAN?

Un **proxy** permite a otros equipos conectarse a una red de forma indirecta a través de él. Cuando un equipo de la red desea acceder a una información o recurso, es realmente el proxy quien realiza la comunicación y a continuación traslada el resultado al equipo inicial. En unos casos esto se hace así porque no es posible la comunicación directa y en otros casos porque el proxy añade una funcionalidad adicional, como puede ser la de mantener los resultados obtenidos.

Por ejemplo: una página web en una caché que permita acelerar sucesivas consultas coincidentes. Con esta denominación general de proxy se agrupan diversas técnicas.

Funcionamiento.

1) El cliente realiza una petición (p. ej. mediante un navegador web) de un recurso de Internet (una página web o cualquier otro archivo) especificado por una URL.

2) Cuando el *proxy* caché recibe la petición, busca la URL resultante en su caché local. Si la encuentra, contrasta la fecha y hora de la versión de la página demanda con el servidor remoto. Si la página no ha cambiado desde que se cargo en caché la devuelve inmediatamente, ahorrándose de esta manera mucho tráfico pues sólo intercambia un paquete para comprobar la versión. Si la versión es antigua o simplemente no se encuentra en la caché, lo captura del servidor remoto, lo devuelve al que lo pidió y guarda o actualiza una copia en su caché para futuras peticiones.

El caché utiliza normalmente un algoritmo para determinar cuándo un documento está obsoleto y debe ser eliminado de la caché, dependiendo de su antigüedad, tamaño e histórico de acceso.

Los ***proxies*** web también pueden filtrar el contenido de las páginas Web servidas. Algunas aplicaciones que intentan bloquear contenido Web ofensivo están implementadas como *proxies* Web. Otros tipos de *proxy* cambian el formato de las páginas web para un propósito o una audiencia específicos, para, por ejemplo, mostrar una página en un teléfono móvil o una PDA. Algunos operadores de red también tienen *proxies para interceptar* virus y otros contenidos hostiles servidos por páginas Web remotas.

Desde el punto de vista del usuario de la red local, el sistema funciona como si tuviera realmente un acceso directo a Internet. El usuario accede inmediatamente desde su ordenador a una página Web o recibe su correo electrónico, sin siquiera saber que el proxy existe.

En realidad, al abrir un programa como Internet Explorer o recoger el correo pendiente, la petición de servicio se realiza al proxy, no al servidor de Internet. El proxy es el encargado de re-direccionar estas peticiones a la máquina correspondiente (el servidor de la página Web o el servidor de correo) y una vez recibida la información, de transmitirla al ordenador que la solicitó.

Ventajas y desventajas de un proxy

a) Ventajas

En general, los proxies hacen posibles varias cosas nuevas:

• **Control**: sólo el intermediario hace el trabajo real, por tanto se pueden limitar y restringir los derechos de los usuarios, y dar permisos sólo al proxy.

• **Ahorro**. Por tanto, sólo *uno* de los usuarios (el proxy) ha de estar equipado para hacer el trabajo real.

• **Velocidad**. Si varios clientes van a pedir el mismo recurso, el proxy puede hacer caché: guardar la respuesta de una petición para darla directamente cuando otro usuario la pida. Así no tiene que volver a contactar con el destino, y acaba más rápido.

• **Filtrado**. El proxy puede negarse a responder algunas peticiones si detecta que están prohibidas.

• **Modificación**. Como intermediario que es, un proxy puede falsificar información, o modificarla siguiendo un algoritmo.

• **Anonimato**. Si todos los usuarios se identifican como uno sólo, es difícil que el recurso accedido pueda diferenciarlos. Pero esto puede ser malo, por ejemplo cuando hay que hacer necesariamente la identificación.

b) Desventajas

En general, el uso de un intermediario puede provocar:

• **Abuso**. Al estar dispuesto a recibir peticiones de muchos usuarios y responderlas, es posible que haga algún trabajo que no toque. Por tanto, ha de controlar quién tiene acceso y quién no a sus servicios, cosa que normalmente es muy difícil.

CUESTIONARIO:

1) ¿Qué tipo de router es el indicado para el uso en una empresa grande?
2) ¿Qué función cumple un router en una red informática?
3) ¿Cómo averiguamos la dirección IP de un router?
4) ¿Se puede cambiar la dirección IP de un router? ¿Cómo se realiza el procedimiento?
5) ¿Qué significa la sigla SSID y qué nos indica?
6) ¿Cómo se realiza el procedimiento para cambiar la contraseña de nuestra red WiFi?
7) ¿Qué función cumple la utilidad DHCP en el router? ¿Cuáles parámetros deben ser configurados?
8) ¿Qué configuración debo hacer en el router para bloquear un dispositivo y que no se pueda conectar a la red WiFi?

Cualquier consulta y la entrega de este trabajo práctico deberán realizarlo a mi casilla de mail davidjim512@hotmail.com
Saludos!!

• **Carga**. Un proxy ha de hacer el trabajo de *muchos* usuarios.
• **Intromisión**. Es un paso más entre origen y destino, y algunos usuarios pueden no querer pasar por el proxy. Y menos si hace de caché y guarda copias de los datos.
• **Incoherencia**. Si hace de caché, es posible que se equivoque y dé una respuesta antigua cuando hay una más reciente en el recurso de destino. En realidad este problema no existe con los servidores proxy actuales, ya que se conectan con el servidor remoto para comprobar que la versión que tiene en cache sigue siendo la misma que la existente en el servidor remoto.
• **Irregularidad**. El hecho de que el proxy represente a más de un usuario da problemas en muchos escenarios, en concreto los que presuponen una comunicación directa entre 1 emisor y 1 receptor (como TCP/IP).

Cualquier consulta y la entrega de este trabajo práctico deberán realizarlo a mi casilla de mail davidjim512@hotmail.com
Saludos!!